#2
PAM
5-29-02

Attorney Docket No. 1602.1006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

J1073 U.S. PTO
10/020434
12/18/01

In re Patent Application of:

Satoshi MUKOGAWA

Application No.: Group Art Unit:

Filed: December 17, 2001 Examiner:

For: INFORMATION PROCESSING APPARATUS AND INPUT OPERATION APPARATUS

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2001-254509

Filed: August 24, 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: December 17, 2001 By: _____
James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

J1073 U.S. PTO
10/020434
12/18/01

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　８月２４日

出願番号
Application Number: 特願２００１－２５４５０９

出願人
Applicant(s): 富士通株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年１０月　４日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０９０８０２

【書類名】　特許願
【整理番号】　0151102
【あて先】　特許庁長官殿
【国際特許分類】　H04K　1/02
　　H04L　9/00
【発明の名称】　情報処理装置及び入力操作装置
【請求項の数】　8
【発明者】
　【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
　【氏名】　向川　聡
【特許出願人】
　【識別番号】　000005223
　【氏名又は名称】　富士通株式会社
【代理人】
　【識別番号】　100097250
　【弁理士】
　【氏名又は名称】　石戸　久子
【選任した代理人】
　【識別番号】　100101856
　【弁理士】
　【氏名又は名称】　赤澤　日出夫
【手数料の表示】
　【予納台帳番号】　038760
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【包括委任状番号】　0014371

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　情報処理装置及び入力操作装置

【特許請求の範囲】

【請求項１】　操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、

前記入力操作部は、前記入力操作部より入力されるデータのうち、暗号化するべきデータを判別する暗号化判別手段と、前記暗号化判別手段の判別結果に基づき、暗号化するべきデータを暗号化する暗号化手段と、暗号化されたデータ、暗号化されないデータの双方を制御部に送信する送信手段とを有し、

前記制御部は、前記入力操作部より受信したデータにつき、暗号化されていないデータの内容に基づいた処理を行うとともに、暗号化されたデータを、復号化機能を有する装置に送信するよう制御することを特徴とする情報処理装置。

【請求項２】　請求項１に記載の情報処理装置において、

前記入力操作部は入力操作用画面を有し、

前記暗号化判別手段は、前記入力操作用画面にて押下された座標が、所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別することを特徴とする情報処理装置。

【請求項３】　請求項２に記載の情報処理装置において、

前記暗号化手段は、前記入力操作用画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする情報処理装置。

【請求項４】　請求項２に記載の情報処理装置において、

前記入力操作用画面における所定の座標範囲又は位置についての情報を外部装置より動的に受信し、設定する設定手段を有し、

前記暗号化判別手段は、前記入力操作用画面にて押下された座標が、前記設定手段で設定された所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別するものであることを特徴とする情報処理装置。

【請求項５】　請求項３に記載の情報処理装置において、

前記入力操作用画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を外部装置より動的に受信し、設定する設定手段を有し、

前記暗号化手段は、前記入力操作用画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする情報処理装置。

【請求項６】　入力操作用画面を有し、該入力操作用画面を通じて操作者より入力された情報を、接続された情報処理装置に提供する入力操作装置であって、

前記入力操作用画面における所定の座標範囲又は位置についての情報、及び座標範囲又は位置において入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を設定する設定手段と、

前記入力操作用画面にて押下された座標が、前記設定手段で設定された所定の座標範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別する暗号化判別手段と、

前記暗号化判別手段により暗号化すべきと判別された入力データにつき、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化する暗号化手段と、

暗号化されたデータ、暗号化されないデータの双方を、接続された情報処理装置に送信する送信手段とを有することを特徴とする入力操作装置。

【請求項７】　操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、

前記入力操作部は、入力された所定のデータを、入力操作部が有する所定のデータと比較する比較手段と、該比較手段により比較された比較結果を前記制御部に送信するための送信手段とを有し、

前記制御部は、受信した比較結果を他の装置に送信するよう制御することを特徴とする情報処理装置。

【請求項８】　操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、

前記入力操作部は、所定のデータを入力する入力動作を検出する検出手段と、所定のデータを暗号化する暗号化手段と、前記検出手段による検出結果及び前記暗号化手段による暗号化データを前記制御部に送信する送信手段とを有し、

前記制御部は、受信した検出結果に基づき、前記入力操作部を制御するとともに、受信した暗号化データを、復号化機能を有する装置に送信するよう制御することを特徴とする情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、入力操作部と制御部を備えた装置に関し、特に、例えば金融機関端末や各種券売機等での入力操作を行う端末等に用いられる装置として、高いセキュリティを有する装置に関するものである。

【０００２】

【従来の技術】

金融機関端末や各種券売機等において、タッチパネル等、画面上に表示されたボタンやポイントを実際に画面に触れる事によって操作する装置があるが、それらの装置にて暗証番号やクレジット番号等、操作者個人の秘密情報を入力する場合がある。また、それらの装置においては通常、入力操作部と装置制御部は一体化されておらず、それぞれがケーブル等で接続されている場合が多い。

【０００３】

図９は、従来これら装置及び装置を含むシステムにおいてセキュリティが保証されていると考えられていた部分を示したブロック図である。本図は入力操作部２と、（装置）制御部３と、その他内部装置６とから構成される装置１、装置１と専用線７で接続された外部機器５から構成されたシステムを示しており、図中の網掛部分がセキュリティが保証されていると考えられていた部分である。従って、入力操作部２から制御部３までのデータの伝達及び制御部３から内部装置６までのデータの伝達は平文（押下位置のポイントデータ等）で送受信されていた

。また、外部機器５に対しても専用線７により平文データで送受信されていた。

【０００４】

【発明が解決しようとする課題】

ところが近年盗聴機器も高性能化してきており、また悪意を持つ者が装置１のメンテナンス作業者や係員になりすますことで不正が行われる場合もあり、必ずしも十分なセキュリティが保たれてはいるとは言えなくなってきた。このため装置１でタッチパネル等から暗証番号等の個人情報が入力された場合、個人情報が漏洩する危険が増大している。従ってこのような盗聴や不正に対応するため、装置内のセキュリティを向上させる必要がでてきている。更に現在、金融機関端末や各種券売機等は様々な場所に設置されているが、その設置場所が無人の場合も多い。またそうした装置の稼働時間も２４時間もしくは深夜までといったように延長される傾向があり、装置における個人情報漏洩を防ぐための高いセキュリティの実現が求められてきている。

【０００５】

装置のセキュリティを保つ手法としては、従来は特開平９－５４８６２号公報や特開２０００－２０４６８号公報で示されるように、画面の覗き込み（盗み見）や動作解析によって前記秘密情報が漏洩する事を防ぐ方法が提案されている程度であるが、これらの手法では画面の操作位置及びキー配列が操作毎に変更されるため、操作者の慣れや利便性を阻害する恐れがある。

【０００６】

また、セキュリティを保証するための単純な方法として、装置１のタッチパネル等での入力の際に、図１０に示すようにタッチパネルで押された座標データをそのまま暗号化し、送信する方法が考えられる。本手法は、入力操作部２で入力された座標データ、例えば（２，７）が入力操作部２の暗号モジュール４で暗号化され、その暗号座標データ「eeff」が制御部３に送信される（Ｓ１）。データを受信した制御部３では暗号座標データの復号化を行い、座標データを画面構成に合わせ数値・文字データもしくは命令指示データに変換する必要がある。本例では数字「４」に変換される。ここで数字「４」について暗号化して外部機器５に送信するべきデータか否かを判別し、暗号化すべきデータと判別されれば数字

「４」を暗号化して、その暗号化電文「0dff」を外部機器５に送信する（Ｓ２）。数字「４」が暗号化すべきデータでない場合は暗号化せず、そのまま制御部内で処理されるか、暗号化しない生データをそのまま外部機器５に送信する、等の通常処理を行う（Ｓ３）。

【０００７】

しかしながら該手法では制御部３でデータの解析を行うため、制御部３に対するセキュリティの保証及び盗聴防止機構（不正防止デバイス化）が必須となる。また制御部３で復号化／暗号化を行うため、復号化／暗号化用のモジュール（暗号モジュール４）も入力操作部２とは別に制御部３内に備えなくてはならない。更にまた暗号化する必要のない通常の制御データも入力操作部２から暗号化されて送信されるため、復号化の処理を行う分処理が増え、装置１に負荷がかかるという問題がある。

【０００８】

本発明は、上述した事情に鑑みてなされたものであって、上記装置１内における個人秘密情報のセキュリティを確保して、他の外部装置へ安全に情報を伝達できる装置を提供する事を目的とする。

【０００９】

【課題を解決するための手段】

上述した課題を解決するため、本発明は操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部は、前記入力操作部より入力されるデータのうち、暗号化するべきデータを判別する暗号化判別手段と、前記暗号化判別手段の判別結果に基づき、暗号化するべきデータを暗号化する暗号化手段と、暗号化されたデータ、暗号化されないデータの双方を制御部に送信する送信手段とを有し、前記制御部は、前記入力操作部より受信したデータにつき、暗号化されていないデータの内容に基づいた処理を行うとともに、暗号化されたデータを、復号化機能を有する装置に送信するよう制御することを特徴とする情報処理装置を提供する。このような情報処理装置は、例えば金融機関等の端末や各種券売機などで使用される装置に適用される。なお、本実施の形態において、復号化機能を有する装置は外

部機器にあたる。

【００１０】

また、前記暗号化手段は、前記入力操作用画面にて押下された座標が、所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判断することを特徴とする。このような構成によれば、例えば入力操作用画面がタッチパネル式の画面である場合、操作者の押下した画面の座標範囲又は位置が例えばセキュリティを要する数字エリアであった場合には暗号化手段が暗号化し、セキュリティを要しない「取り消し」や「確認」のための入力エリアであった場合には暗号化しない等、場合に応じた対応が可能となり、効率よく処理することができる。

【００１１】

更に、前記暗号化手段は、前記入力操作用画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする。具体的には、例えば上記と同様入力操作用画面がタッチパネル式の画面である場合、操作者の押下した座標範囲や位置が数字エリアに相当する座標範囲や位置であった場合には該当の数字に変換するよう暗号化手段が機能する。更に変換された数字がセキュリティを要する場合には暗号化処理を行う。このような構成によれば、入力操作部で入力された様々なデータを適切なデータ情報に変換して利用することができ、さらに暗号化することでセキュリティを確実に確保することができる。

【００１２】

更に、本発明に係る情報処理装置は、前記入力操作用画面における所定の座標範囲又は位置についての情報を外部装置より動的に受信し、設定する設定手段を有し、前記暗号化判別手段は、前記入力操作用画面にて押下された座標が、前記設定手段で設定された所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別するものであることを特徴とする。このような構成によれば、例えば入力操作用画面がタッチパネル式画面である場合、タッチパネル画面のレイアウト等のような座標範囲や位置の情報を外部装置から受信し、

受信したデータに基づいて画面の設定を行うことができるため、様々なパターンでタッチパネルの表示を行うことができる。さらにそのようなレイアウトの情報に応じて暗号化の判別を行うことにより、様々なパターンに応じて暗号化処理を効率的に行うことが可能となる。

【００１３】

更に又、本発明に係る情報処理装置において、前記入力操作用画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を外部装置より動的に受信し、設定する設定手段を有し、前記暗号化手段は、前記入力操作用画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする。データ設定情報は、本発明の実施の形態４においては座標範囲及び関連データコードとの対応を示す座標情報（図５）により構成される。暗号化手段（実施の形態ではデータ処理部）は、該座標情報を用いてタッチパネルより入力されたデータを関連データコードに変換し、暗号化する。

【００１４】

このような構成によれば、入力操作部の座標範囲や位置に対応して様々なデータを割り当てることができ、セキュリティを要する装置にあっては入力操作用画面に対し多種多様な状況に応じた設定を施すことが可能となる。さらに該設定に応じて暗号化の処理がなされるため、従来に比して柔軟性高く、セキュリティを確保することができる。

【００１５】

また、本発明は、入力操作用画面を有し、該入力操作用画面を通じて操作者より入力された情報を、接続された情報処理装置に提供する入力操作装置であって、前記入力操作用画面における所定の座標範囲又は位置についての情報、及び座標範囲又は位置において入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を設定する設定手段と、入力操作用画面にて押下された座標が、前記設定手段で設定された所定の座標範囲又

は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別する暗号化判別手段と、前記暗号化判別手段により暗号化すべきと判別された入力データにつき、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化する暗号化手段と、暗号化されたデータ、暗号化されないデータの双方を、接続された情報処理装置に送信する送信手段とを有することを特徴とする入力操作装置を提供する。このような入力操作装置をセキュリティを要する金融機関等のシステムや各種券売機等の装置に設けることにより、従来に比してセキュリティが強化され、情報の漏洩を防止することができる。

【００１６】

また、本発明は操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部は、入力された所定のデータを、入力操作部が有する所定のデータと比較する比較手段と、該比較手段により比較された比較結果を前記制御部に送信するための送信手段とを有し、前記制御部は、受信した比較結果を他の装置に送信するよう制御することを特徴とする。本発明の実施の形態では、入力操作部の内部メモリに予め会員番号の比較検証のための比較データを記憶しておき、例えば利用者が会員番号等をタッチパネルにて入力する際、その比較データと利用者により入力された会員番号を入力操作部にて比較検証して、その利用者が会員として登録されているか否かを判断するようにしている。

【００１７】

このような構成によれば、利用者が装置に対して入力した個人情報が外部に漏洩せず、セキュリティを確保できる。更に、入力されたデータについては入力操作部にて暗号化すべきか否かの判断がなされるため、暗号化及び復号化の処理を制御部で行う必要がなくなり、又装置内で行われる暗号化・復号化の処理を軽減することができる。これにより装置の負荷が軽減する。

【００１８】

更に、本発明は、操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部

は、所定のデータを入力する入力動作を検出する検出手段と、所定のデータを暗号化する暗号化手段と、前記検出手段による検出結果及び前記暗号化手段による暗号化データを前記制御部に送信する送信手段とを有し、前記制御部は、受信した検出結果に基づき、前記入力操作部を制御するとともに、受信した暗号化データを、復号化機能を有する装置に送信するよう制御することを特徴とする。

【００１９】

例えば、一般的に金融機関等の端末のような装置において暗証番号の入力を行う場合、入力された番号自体は画面に表示されず、入力された旨を示す記号（例えば「＊」）のみが各数字が入力される度に表示されるようになっている。この場合、従来では入力操作部が押下された座標データを暗号化する等して制御部に送信することで制御部が入力動作を検出し表示画面を制御していたが、本発明に係る実施の形態では、入力操作部にて入力動作を検出するようにし、入力操作部から制御部に対して暗証番号の入力動作があったことのみを通知するだけで、制御部が表示画面を制御できるようにし、更に全ての暗証番号の数字の入力が完了した場合には、その暗証番号を暗号化して制御部に送信するようにしたため、従来に比して暗号化等の手間が省け、セキュリティも向上する。

【００２０】

【発明の実施の形態】

以下、図を用いて、本発明の実施の形態を詳細に説明する。

実施の形態１．

図１は、本発明の一実施の形態における基本構成及びセキュリティ保証のための基本手法を簡便に表したブロック図である。上述した図１０による手法と比較するため、図１０と同様のデータを用いて説明する。図において、装置１０は図１０における装置１と同様に入力操作部２０及び制御部３０から構成され外部機器５０に接続されている。

【００２１】

本手法は、まず入力操作部２０でタッチパネルなどにより座標データ、例えば（２，７）が入力されると、押下座標（２，７）を関連データに変換する。ここでいう関連データとは、タッチパネルで押下された座標上に表示された数字など

の文字や記号等をいう。ここで関連データが数字「４」であるとすると、入力操作部２０において数字「４」が暗号化すべきデータか否かを判断し、暗号化すべきデータであると判断された場合には、入力操作部２０の暗号モジュール２４で数字「４」が暗号化され、その暗号化電文「0dff」が制御部３０に送信される（Ｓ１ａ）。制御部３０では受信したデータが暗号化電文であれば、何も処理を行わず受信した暗号化電文そのままを外部機器５０に送信する（Ｓ１ｂ）。

【００２２】

また、同様に、入力操作部２０で座標データ（２，７）が入力されると、押下座標（２，７）の変換された関連データが暗号化されるべきデータか否かを判断し、暗号化しなくてもよい、所謂平文で通信が可能であるデータだと判断された場合には、平文で座標データ（２，７）がそのまま制御部３０に送信され（Ｓ２ａ）、通常処理される（Ｓ２ｂ）。

【００２３】

このような手法を用いることにより、特に、図９に示された装置１のように装置１全体もしくは入力操作部２と制御部３を一体化し、不正防止デバイスとしてセキュリティを確保できない場合、及び、物理的に入力操作部２とセキュリティを必要とされるデバイスが離れている場合であっても、本実施の形態に示された入力操作部２０のように、暗号化すべきデータの識別機能を有していさえすれば、制御部３に暗号モジュール４を備える必要もなく、セキュリティを容易に確保できる。

【００２４】

実施の形態２．

図２は本発明における実施の形態２の基本構成を示すブロック図である。図に示されるように、金融機関端末や各種券売機等の装置１０は、利用者の入力操作コントロール及び暗号化やデータ送信等を行う入力操作部２０及び装置１０全体の制御を行いＩＣカード等のセキュリティが保証されたデバイス（セキュリティモジュール）４０や外部機器５０に対してデータの送信を行う制御部３０から構成される。

【００２５】

入力操作部２０は、タッチパネル等の入力部２１、入力部２１による入力を制御する入力部コントローラ２２，入力部コントローラ２２から入力データを受け取り座標データを所定のデータに変換したり暗号化のための符号化やブロック化を行うデータ処理部２３、データ処理部から受け取ったデータを暗号化する暗号モジュール２４，各種データを保存する内部メモリ２５、制御部３０とのデータの送受信を行う送受信部２６から構成される。

【００２６】

制御部３０は、入力操作部２０やセキュリティモジュール４０や外部機器５０とのデータの送受信を行うための送受信部３１、送受信部３１により受信された座標データを所定のデータに変換するデータ変換部３２，入力部２１の画面制御を行う画面表示制御部３３から構成される。

また、図中の入力操作部２０をはじめとする網掛部分はセキュリティが保証されているモジュール（不正防止デバイス）とする。

【００２７】

図３は、画面表示制御部３３により制御されるタッチパネル式入力画面の表示例である。図中の網掛部分は利用者が暗証番号や金額等を入力する際に触れる数字エリア２１ａであり、ここで入力されるデータはセキュリティが保証されるようにしている。また、本画面はそうしたセキュリティエリア２１ａの他に、利用者が入力操作を行った場合、その入力動作を利用者が確認できるよう「＊」のような所定の文字等が表示されるエリア２１ｂと、利用者が行った入力操作を取り消すためのエリア２１ｃと、入力操作をやり直すためのエリア２１ｄを備えている。

【００２８】

このような構成に基づき、以下、図４のフローチャートを用いて暗号化処理についての詳細を説明する。本実施の形態では、利用者が装置１０に対して個人の秘密情報の１つである４桁の暗証番号を入力する処理を行い、入力データのまま、もしくは符号化或いはブロック化して暗号化し、不正防止デバイスである外部機器５０或いはセキュリティモジュール４０まで送信する例を説明する。

【００２９】

まず、装置１０の制御部３０の画面表示制御部３３により図３に示されるような画面を表示する（Ｓ４００）。また、図３の画面においてセキュリティが必要な座標範囲部分（２１ａ）の情報を別途外部機器５０から動的にデータとして受信し通知され、座標範囲指定及び関連データコードを設定する（Ｓ４０１）。この場合の関連データコードは便宜的にそれぞれ数字とする。例えば１が表示されている座標範囲（１０～２０，２０～４０）がポイントされた場合はコード「１」、５が表示されている座標範囲（２０～３０，４０～８０）がポイントされた場合はコード「５」とする。このような設定は内部メモリ２５に格納される。

【００３０】

図５は、受信された座標情報の一例を示すものである。受信された情報は暗号化されていても良く、暗号化されていた場合には（Ｓ４０２、Ｙ）、入力操作部２０の暗号モジュール２４において復号化され使用される（Ｓ４０３）。また、暗号化されていない場合には（Ｓ４０２、Ｎ）、受信された情報そのままを使用する。このように本実施の形態では、セキュリティを要する座標の情報を外部機器５０から受信するようにしたが、予め入力操作部２０の内部メモリ２５に静的に記憶しておいてもよい。

【００３１】

ここで利用者が図３のように表示された画面から入力部２１により暗証番号を入力する操作を行う。入力操作を行うと、入力データは入力部コントローラ２２に通知され、座標データに変換される。この入力操作によりセキュリティが必要な情報以外の座標がポイントされた場合は（Ｓ４０４、Ｙ）、通常通り制御部３０に座標情報をそのまま通知し処理を行う。具体的には、例えば利用者が（６０，８０）の座標を押下したとすると、入力部コントローラ２２により、押下された座標は図３に示されたセキュリティを要する座標範囲（数字エリア２１ａ）内ではないと判断され、座標情報をそのまま制御部３０に通知する（Ｓ４０５）。制御部３０では送受信部３１による受信した座標データをデータ変換部３２にて関連データに変換し、ポイントされた位置の関連データが、例えば「取消」処理であれば（Ｓ４０６、Ｙ）、入力処理自体を終了する等（Ｓ４０７）、「やり直し」であれば（Ｓ４０６、Ｎ）、保持されている内部メモリ２５内のデータを削

除し最初から入力させる等の処理を行う。

【００３２】

また、セキュリティが必要な情報の座標がポイントされた場合は（Ｓ４０４、Ｎ、及び、Ｓ４０８、Ｙ）、座標情報の代わりに入力通知のみを知らせるコードを制御部３０に通知する（Ｓ４０９）。通知を受けた制御部３０は、利用者に対して、画面上に入力桁数がわかるように「＊」のような文字を図３の表示エリア２１ｂに表示させるのと同時に、入力を知らせる音等で通知する制御を行う。また、データ処理部２３は内部メモリ２５に格納された図５の情報を参照してポイントされた座標を関連データコードに変換し、変換結果を内部メモリ２５内に格納する。例えば、利用者により（１５，３０）の座標が入力されたとすると、関連データコード「１」が格納される。利用者の暗証番号入力が終了しない間は（Ｓ４１０、Ｎ）、Ｓ４０４からＳ４１０の処理を繰り返す。

【００３３】

セキュリティが必要な情報の座標が４点入力されると、暗証番号の入力が終了したとして（Ｓ４１０、Ｙ）、データ処理部２３は内部メモリ２５内にあるコード情報を編集してブロック化し（Ｓ４１１）、暗号モジュール２４にて暗号化し（Ｓ４１２）、送受信部２６により制御部３０に送信する（Ｓ４１３）。なお、ブロック化を、例えばコードを入力順に上位の桁に当てはめ、入力されていないコードを「０」として８桁のブロック化を行うようにしてもよい。この場合、例えばコード「１」、「２」、「３」、「４」の順でポイントされたデータは、「１２３４００００」となる。

【００３４】

もちろん、このブロック化を必ず行う必要はなく、符合化したり、また何の処理もせず暗号化のみを行うようにしてもよく、その処理は限定されない。

暗号化は、内部メモリ２５内に記憶してある鍵を使用して行われる。送信された暗号化データは制御部３０を通じて、セキュアな外部機器５０或いはセキュリティモジュール４０まで送信される。この際制御部３０で本暗号化データが解析される事はない。

【００３５】

実施の形態３．

本実施の形態の基本構成は、実施の形態２で示された図２と同様である。また、本実施の形態では、８桁の会員番号入力処理を行い、番号を入力操作部２０において比較・確認することにより、会員として登録されているかどうかを検証する例を用いる。従って、本実施の形態では、内部メモリ２５内には、利用者により入力された会員番号を比較・確認するための比較データが予め格納されているか、もしくは暗号化された比較データを外部装置５０から動的に受信するものとする。更に、本実施の形態では、予め座標範囲／位置とそれに関連するデータを複数パターン内部メモリ２５に格納しておき、本パターンを表示画面にあわせて装置１０の管理者が任意に選択できるものとする。

【００３６】

図６は、本実施の形態における会員番号入力処理の詳細を示したフローチャートである。まず、装置１０の制御部３０の画面表示制御部３３により会員番号入力用の画面を表示する（Ｓ６００）。図７（ａ）は本実施の形態における会員番号入力用画面の表示例である。また、図５に示されるような座標範囲部分及びそれに対応する関連データコードの情報を予め複数パターン内部メモリ２５に登録しておく。図７（ｂ）、（ｃ）、（ｄ）は登録されたパターンの例であり、この場合３パターン登録されているものとする。図において網掛部分がセキュリティを要する入力エリアである。

【００３７】

次に装置１０の管理者が、図７（ａ）の画面におけるセキュリティが必要な座標範囲部分情報に合致するパターンを、登録してあるパターン（図７（ｂ）、（ｃ）、（ｄ））から選択し、座標範囲指定及び関連データコードを設定する。この場合図７（ｂ）のパターン１を選択する（Ｓ６０１）。パターン選択のための画面は、画面表示制御部３３により管理者用の設定入力画面が別途用意されており、その設定入力画面にて行う（図示せず）。また、選択されたパターンによる座標範囲指定及び関連データコードの設定は、実施の形態２と同様に行われているものとする。本設定に基づいて、入力された座標データがセキュリティを要するか否かが判断され、その判断に基づいて処理される。

【００３８】

具体的には、まず、利用者が図７（ａ）の入力画面から会員番号を入力する操作を入力部２１により行う。入力操作を行うと、入力データは入力部コントローラ２２に通知され、座標データに変換される。変換された座標データがセキュリティ確保の必要があるデータか否かを入力部コントローラ２２が上記設定に従って判断し、セキュリティが必要な情報以外の座標がポイントされた場合は（Ｓ６０２、Ｙ）、通常通り制御部３０に座標情報をそのまま通知し（Ｓ６０３）、処理を行う。その処理（Ｓ６０４からＳ６０５）は、実施の形態２と同様であるため説明を省略する。

【００３９】

また、セキュリティが必要な情報の座標がポイントされた場合（Ｓ６０２、Ｎ、及び、Ｓ６０６、Ｙ）の処理（Ｓ６０７）も実施の形態２と同様であり、ポイントされた座標に対応した関連データコードを内部メモリ２５内に格納する。利用者の会員番号入力が終了しない間は（Ｓ６０８、Ｎ）、Ｓ６０２からＳ６０８の処理を繰り返す。

【００４０】

セキュリティが必要な情報の座標が８点入力されると（例えば、ここでは便宜的に会員番号「ＤＦ８－５２２０」が入力されたものとする。）、会員番号の入力が終了したとして、データ処理部２３は、内部メモリ２５内に静的に比較データが存在する場合には（Ｓ６０８、Ｙ、静的）内部メモリ２５内にある比較データを用いて、入力されたデータとの比較を行う（Ｓ６０９）。また、動的に受信した暗号化された比較データを用いる場合には（Ｓ６０８、Ｙ、動的）、受信した暗号化データを復号化し比較する方法（Ｓ６１０）もしくは、入力されたデータを暗号化して比較する方法（Ｓ６１１）を用いて比較を行う。入力データを暗号化する方法は、内部メモリ２５に受信した比較データを暗号化した鍵と同じ暗号化鍵を予め記憶しておき、それを用いて暗号化する。比較する方法はいずれを用いてもよく、特に限定されない。

【００４１】

以下、比較処理の例を示す。

１．静的に内部メモリに記憶された比較データを用いる場合（Ｓ６０９）

入力データ：ＤＦ８－５２２０

↓　（比較）　－－－－＞　ＯＫ

比較データ：ＤＦ８－５２２０

【００４２】

２．動的に受信した比較データを復号化して用いる場合（Ｓ６１０）

入力データ：ＤＦ８－５２２０

↓　（比較）　－－－－＞　ＯＫ

比較データ復号化：ＤＦ８－５２２０

↑　（復号化）

受信比較データ：２３４８８９０２２１３

【００４３】

３．動的に受信した比較データを用いるが、入力されたデータの方を暗号化して比較する場合（Ｓ６１１）

入力データ：ＤＦ８－５２２０

↓　（暗号化）

入力データ暗号化：２３４８８９０２２１３

↓　（比較）　－－－－＞　ＯＫ

受信比較データ：２３４８８９０２２１３

【００４４】

このように比較検証された結果は、制御部３０或いは制御部３０を通して外部機器５０やセキュリティモジュール４０に通知される（Ｓ６１２）。具体的には、同一であれば（上記ＯＫ）、送受信部２６より送信データとして検証成功コードを送信する。もし相違があれば、送受信部２６より送信データとして検証失敗コードを送信する。従って本実施の形態では、入力されたデータは入力操作部２０内にて処理され、外部には検証結果のみが通知される。

【００４５】

実施の形態４．

本実施の形態の基本構成は、実施の形態２で示された図２と同様である。また

、画面表示例は、図７（ａ）の画面表示例と同様であるとする。本実施の形態では、装置１０の管理者が１６桁の暗号化／復号化用の鍵の入力処理を行い、入力された暗号鍵を用いて暗号化したデータを送信する例を用いる。

【００４６】

図８は、本実施の形態における暗号化用鍵入力処理の詳細を示したフローチャートである。まず、装置１０の制御部３０の画面表示制御部３３により暗号化用鍵入力用の画面を表示する（Ｓ８００）。また、実施の形態２と同様に、別途外部機器５０から動的に座標範囲指定及び関連データコードの情報を受信し、設定する（Ｓ８０１～Ｓ８０３）。

【００４７】

さらに、実施の形態２と同様に、まず、管理者が図７（ａ）の入力画面から入力部２１により暗号化用鍵を入力する操作を行う。この入力操作から入力が終了するまでのフロー（Ｓ８０４～Ｓ８１０）は実施の形態２と同様であるため説明を省略する。

【００４８】

セキュリティが必要な情報の座標が１６点入力されると（例えば、ここでは便宜的に暗号化／復号化用の鍵「０１２３４５６７８９ＡＢＣＤＥＦ」が入力されたものとする。）、入力部コントローラ２２により内部メモリ２５内に格納される（Ｓ８１１）。格納された暗号化／復号化用の鍵を用いて、暗号モジュール２４により内部メモリ２５内に記憶されたデータもしくは外部機器５０から動的に受信したデータの暗号化を行う（Ｓ８１２）。暗号化の例を下記に示す。

【００４９】

内部メモリ２５内のデータ：４０２９３３

（動的受信データ：４０２９３３）

↓　（入力鍵：０１２３４５６７８９ＡＢＣＤＥＦによる暗号化）

暗号化データ：９Ａ２３４ＤＦ１２３１０２ＡＥＦ

暗号化され制御部３０に送信された暗号化データは、制御部３０からセキュアな外部機器５０或いはセキュリティモジュール４０まで送信される（Ｓ８１３）。

なお、暗号化の方法自体は本発明の目的の範囲ではないので、ここでの詳細な説明は省略する。

【００５０】

また、本実施の形態により入力され格納された暗号化／復号化用の鍵は、上述した全ての実施の形態において利用可能である。

【００５１】

以上、本発明の様々な実施の形態を説明したが、本発明は上述した実施の形態に限定されることはなく、本発明の要旨を逸脱しない範囲において適用可能であることはもちろんである。

【００５２】

（付記１）操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部は、前記入力操作部より入力されるデータのうち、暗号化するべきデータを判別する暗号化判別手段と、前記暗号化判別手段の判別結果に基づき、暗号化するべきデータを暗号化する暗号化手段と、暗号化されたデータ、暗号化されないデータの双方を制御部に送信する送信手段とを有し、前記制御部は、前記入力操作部より受信したデータにつき、暗号化されていないデータの内容に基づいた処理を行うとともに、暗号化されたデータを、復号化機能を有する装置に送信するよう制御することを特徴とする情報処理装置。

（付記２）付記１に記載の情報処理装置において、前記入力操作部は入力操作用画面を有し、前記暗号化判別手段は、前記入力操作用画面にて押下された座標が、所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別することを特徴とする情報処理装置。

（付記３）付記２に記載の情報処理装置において、前記暗号化手段は、前記入力操作用画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする情報処理装置。

（付記４）付記２に記載の情報処理装置において、前記入力操作用画面における所定の座標範囲又は位置についての情報を外部装置より動的に受信し、設定する

設定手段を有し、前記暗号化判別手段は、前記入力操作用画面にて押下された座標が、前記設定手段で設定された所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別するものであることを特徴とする情報処理装置。

（付記５）付記３に記載の情報処理装置において、前記入力操作用画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を外部装置より動的に受信し、設定する設定手段を有し、前記暗号化手段は、前記入力操作用画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする情報処理装置。

（付記６）入力操作用画面を有し、該入力操作用画面を通じて操作者より入力された情報を、接続された情報処理装置に提供する入力操作装置であって、前記入力操作用画面における所定の座標範囲又は位置についての情報、及び座標範囲又は位置において入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を設定する設定手段と、前記入力操作用画面にて押下された座標が、前記設定手段で設定された所定の座標範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別する暗号化判別手段と、前記暗号化判別手段により暗号化すべきと判別された入力データにつき、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化する暗号化手段と、暗号化されたデータ、暗号化されないデータの双方を、接続された情報処理装置に送信する送信手段とを有することを特徴とする入力操作装置。

（付記７）操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部は、入力された所定のデータを、入力操作部が有する所定のデータと比較する比較手段と、該比較手段により比較された比較結果を前記制御部に送信するための送信手段とを有し、前記制御部は、受信した比較結果を他の装置に送信するよう制御する

ことを特徴とする情報処理装置。

（付記８）操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部は、所定のデータを入力する入力動作を検出する検出手段と、所定のデータを暗号化する暗号化手段と、前記検出手段による検出結果及び前記暗号化手段による暗号化データを前記制御部に送信する送信手段とを有し、前記制御部は、受信した検出結果に基づき、前記入力操作部を制御するとともに、受信した暗号化データを、復号化機能を有する装置に送信するよう制御することを特徴とする情報処理装置。

（付記９）付記３に記載の情報処理装置において、前記暗号化手段は、前記入力操作用画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換すると共に、該データ情報を符合化もしくはブロック化し、該符合化もしくはブロック化されたデータを所定の鍵を使用して暗号化することを特徴とする情報処理装置。

（付記１０）付記７に記載の情報処理装置において、前記入力操作部には、前記入力操作部より入力されるデータのうち、前記比較手段により比較するべきデータを判別する比較判別手段を備え、前記比較手段は前記比較判別手段により判別されたデータを比較することを特徴とする情報処理装置。

（付記１１）付記７に記載の情報処理装置において、前記入力操作部が有する所定のデータは、前記入力操作部が有するメモリ内に記憶されていることを特徴とする情報処理装置。

（付記１２）付記７に記載の情報処理装置において、前記入力操作部が有する所定のデータは、外部装置から暗号化されて送られる受信データに基づくデータであることを特徴とする情報処理装置。

（付記１３）付記１２に記載の情報処理装置において、前記暗号化されたデータを復号する復号化手段を備えていることを特徴とする情報処理装置。

（付記１４）付記１２又は付記１３に記載の情報処理装置において、前記入力操作部は、前記入力操作部より入力されたデータを、前記外部装置から暗号化されて送られる前記受信データが暗号化されたものと共通の鍵により暗号化する手段

を有し、前記比較手段は、これら暗号化されているデータを比較することを特徴とする情報処理装置。

（付記１５）付記１０に記載の情報処理装置において、前記入力操作部は入力操作用画面を備え、前記比較判別手段により判別が行われて前記比較手段により比較処理が行われるデータは、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力され、その座標範囲又は位置に関連付けられるデータであることを特徴とする情報処理装置。

（付記１６）付記５に記載の情報処理装置において、前記外部装置から受信される前記データ設定情報は暗号化されており、前記入力操作部には、該暗号化された前記データ設定情報を復号化する手段を有することを特徴とする情報処理装置。

（付記１７）付記５に記載の情報処理装置において、互いに異なる複数の前記データ設定情報を記憶する記憶手段を有し、前記入力操作用画面において、前記複数の設定情報の中から所定のデータ設定情報を選択して設定できる手段を有することを特徴とする情報処理装置。

（付記１８）付記１乃至付記５又は付記１３のいずれかに記載の情報処理装置において、前記データを暗号化するための鍵、及びデータを必要に応じて復号化するための鍵は、前記入力操作部により入力された所定のデータに基づいて形成されることを特徴とする情報処理装置。

（付記１９）付記１乃至付記５又は付記７乃至付記１８のいずれかに記載の情報処理装置において、前記入力操作部は不正防止デバイスで構成されていることを特徴とする情報処理装置。

（付記２０）付記１乃至付記５又は付記７乃至付記１９のいずれかに記載の情報処理装置において、前記所定のデータは、セキュリティを要求されるデータであり、暗証番号やクレジット番号等、操作者個人の秘密情報、又は暗号化／復号化用の鍵等のデータの少なくともいずれかが含まれることを特徴とする情報処理装置。

【００５３】

【発明の効果】

以上説明したように、本発明は、入力操作部と制御部を有する装置において、入力操作部に入力されたデータを暗号化する暗号モジュールと外部機器に送信するための送受信部を備えたため、不正防止デバイスとして入力操作部と制御部が一体化できない場合や、物理的に入力操作部とセキュリティを要するデバイスが離れている場合であっても、個人情報が漏洩せず、セキュリティを確保できる。更にまた、本発明は、入力操作部に入力されたデータを暗号化すべきか否かを判別するための機能を設けたことにより、制御部は入力操作部から受信したデータについて暗号化及び復号化の処理を行う必要がなくなり、装置内で行われる暗号化・復号化の処理を軽減することができるため、装置の負荷が軽減する。また、従来の装置を使用する場合においても、装置制御部側の変更を要せず、入力操作部の交換のみで対応できるため、既存設置装置に対しても導入コストの低減を計る事ができ、装置におけるセキュリティが大幅に向上する。

【図面の簡単な説明】

【図１】

本発明の実施の形態１における基本構成及びセキュリティ保証のための基本手法を簡便に表したブロック図である。

【図２】

本発明における実施の形態２乃至実施の形態４の基本構成を示すブロック図である。

【図３】

タッチパネル式入力画面の表示例である。

【図４】

実施の形態２における暗号化処理のフローチャートである。

【図５】

セキュリティが必要な座標範囲とそれに対応する関連データの一例である。

【図６】

実施の形態３における会員番号入力処理のフローチャートである。

【図７】

（ａ）実施の形態３及び実施の形態４における入力用画面の表示例である。

（ｂ）、（ｃ）、（ｄ）は実施の形態２における登録された座標範囲部分及びそれに対応する関連データコードの情報のパターンの例である。

【図８】

実施の形態４における暗号化用鍵入力処理の詳細を示したフローチャートである。

【図９】

従来セキュリティが保証されていると考えられていた部分を示したブロック図である。

【図１０】

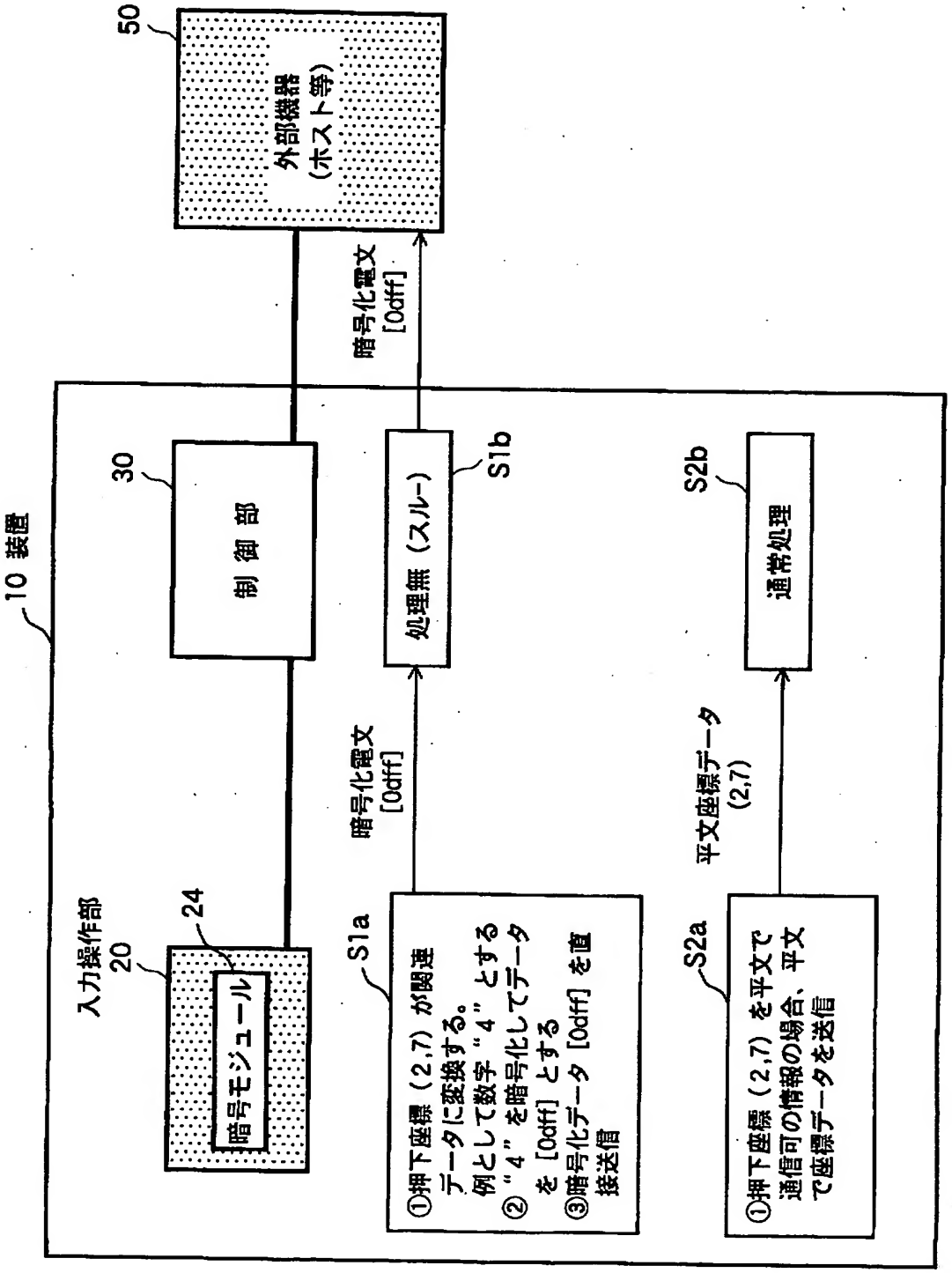
タッチパネルで押された座標データをそのまま暗号化し、送信する手法を示したブロック図である。

【符号の説明】

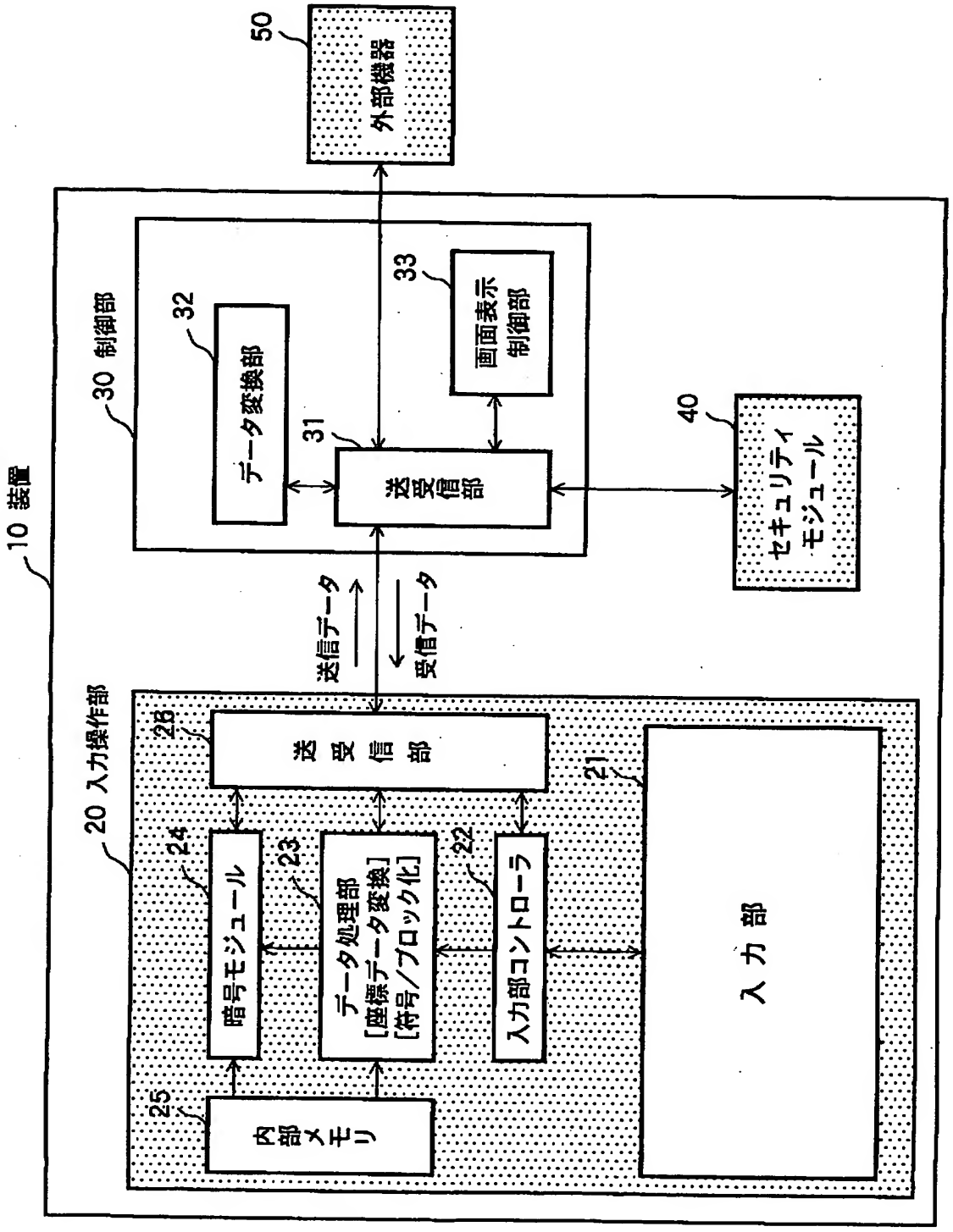
１０　装置、２０　入力操作部、２１　入力部、２２入力部コントローラ、２３　データ処理部、２４　暗号モジュール、２６　送受信部、３０　制御部、３１　送受信部、３２　データ変換部、３３　画面表示制御部、４０　セキュリティモジュール、５０　外部機器。

【書類名】　　図面

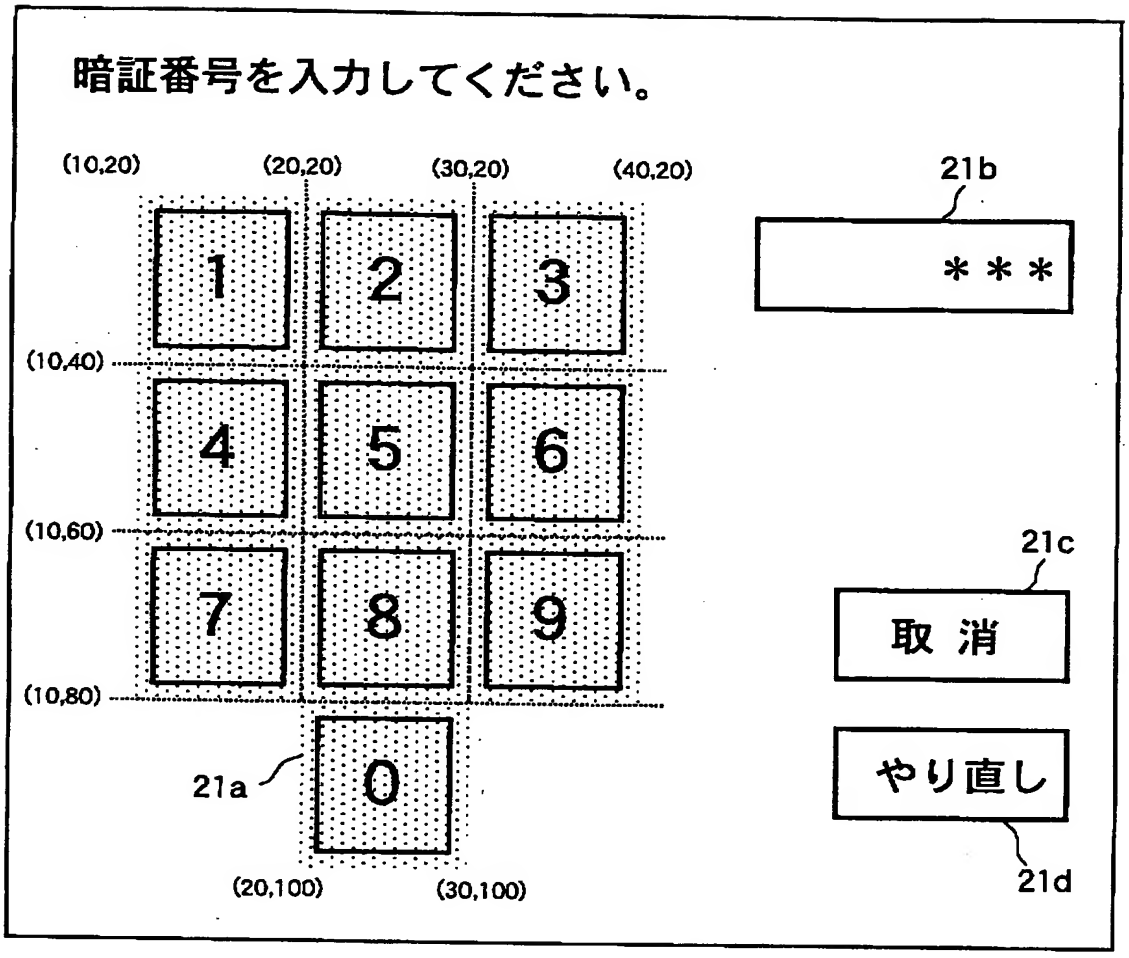
【図１】


50
外部機器
(ホスト等)
暗号化電文
[Odff]
10 装置
30
制御部
処理無（スルー）
S1b
S2b
通常処理
入力操作部
20
24
暗号モジュール
暗号化電文
[Odff]
平文座標データ
(2,7)
S1a
①押下座標（2,7）が関連
データに変換する。
例として数字“4”とする
②“4”を暗号化してデータ
を[Odff]とする
③暗号化データ[Odff]を直
接送信
S2a
①押下座標（2,7）を平文で
通信可の情報の場合、平文
で座標データを送信

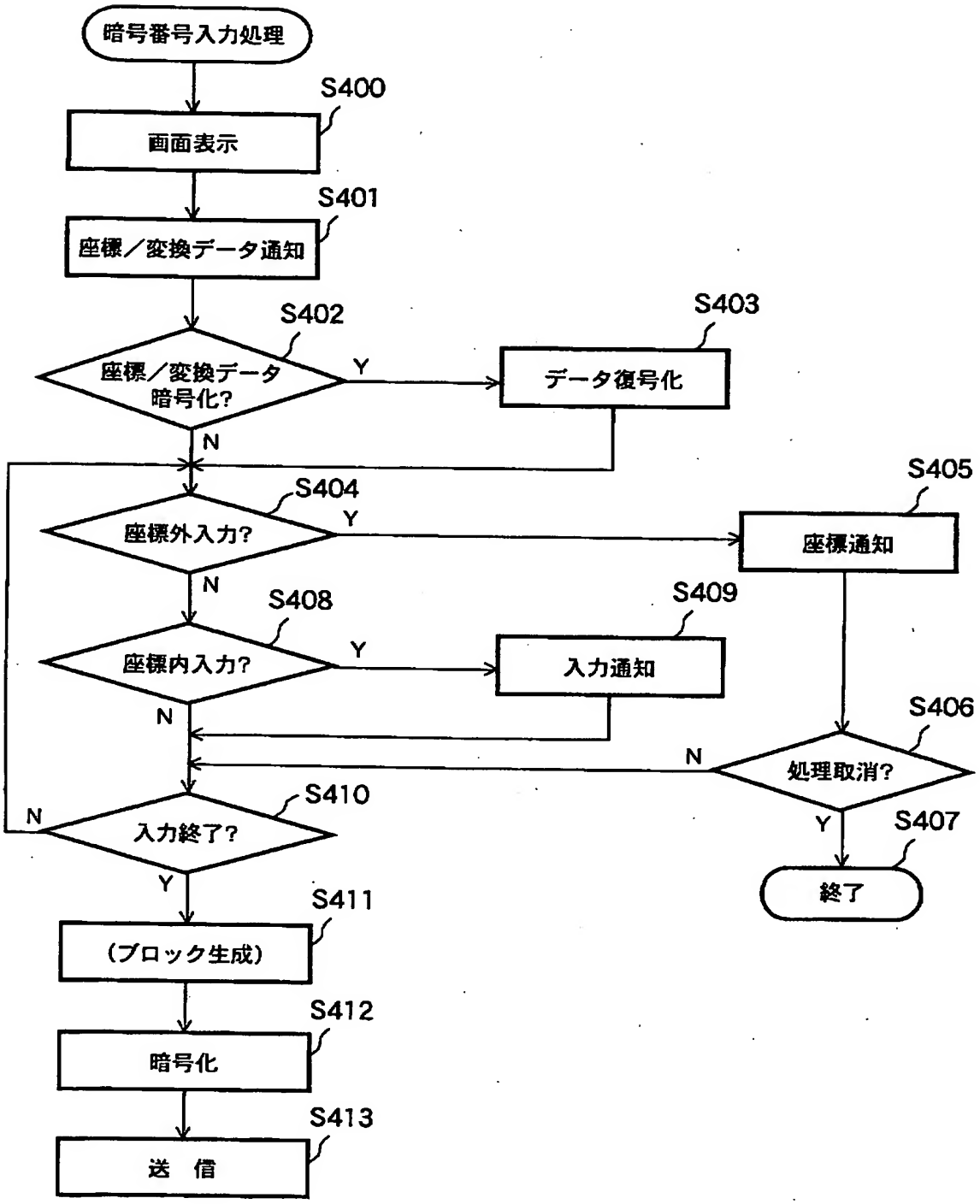
【図２】


50
外部機器
10 装置
30 制御部
32
データ変換部
33
画面表示制御部
31
送受信部
40
セキュリティモジュール
送信データ
受信データ
20 入力操作部
26
送受信部
21
24
暗号モジュール
23
データ処理部
[座標データ変換]
[符号／ブロック化]
22
入力部コントローラ
入力部
25
内部メモリ

【図３】


暗証番号を入力してください。
(10,20)
(20,20)
(30,20)
(40,20)
(10,40)
(10,60)
(10,80)
(20,100)
(30,100)
1
2
3
4
5
6
7
8
9
0
21a
21b
＊＊＊
21c
取 消
やり直し
21d

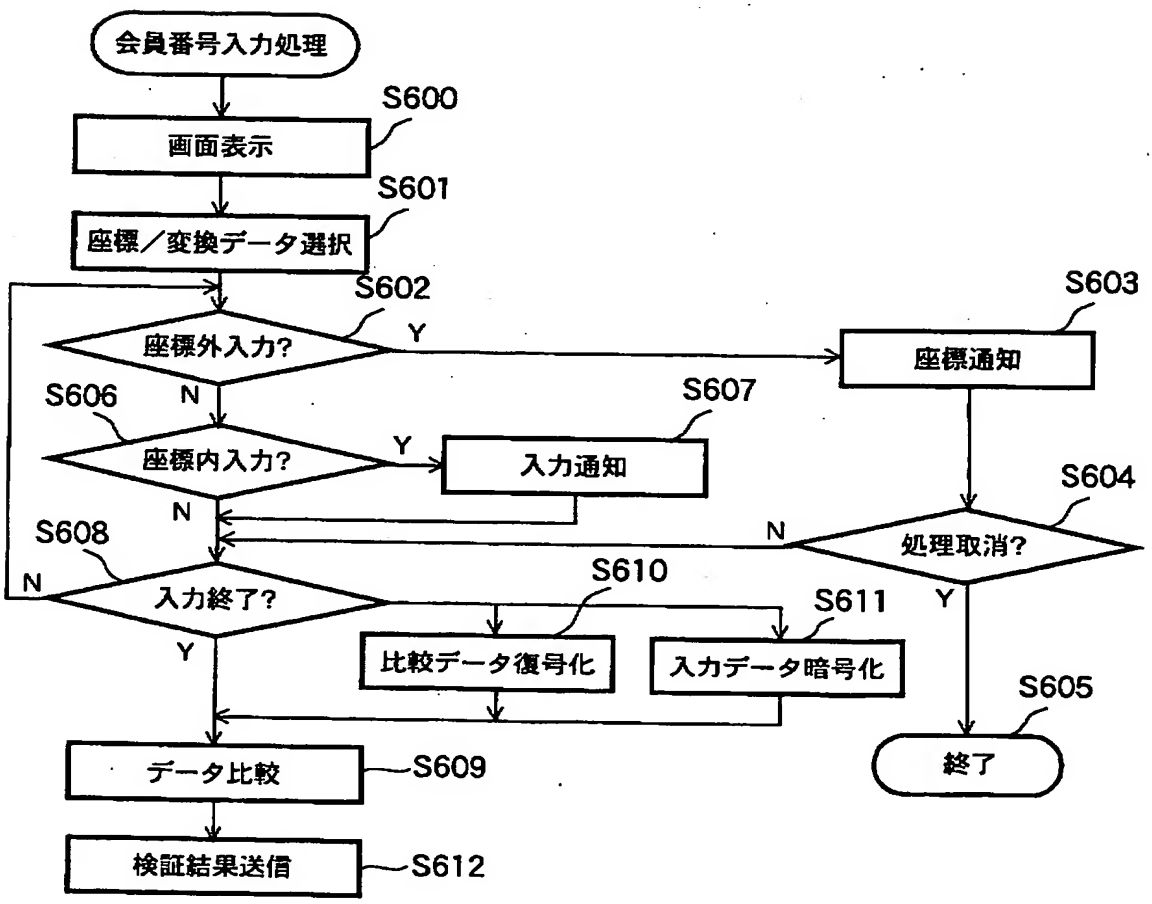
【図４】


暗号番号入力処理
S400
画面表示
S401
座標／変換データ通知
S402
座標／変換データ暗号化?
Y
S403
データ復号化
N
S404
座標外入力?
Y
S405
座標通知
N
S408
座標内入力?
Y
S409
入力通知
N
S406
処理取消?
N
S410
入力終了?
N
Y
S407
終了
Y
S411
(ブロック生成)
S412
暗号化
S413
送　信

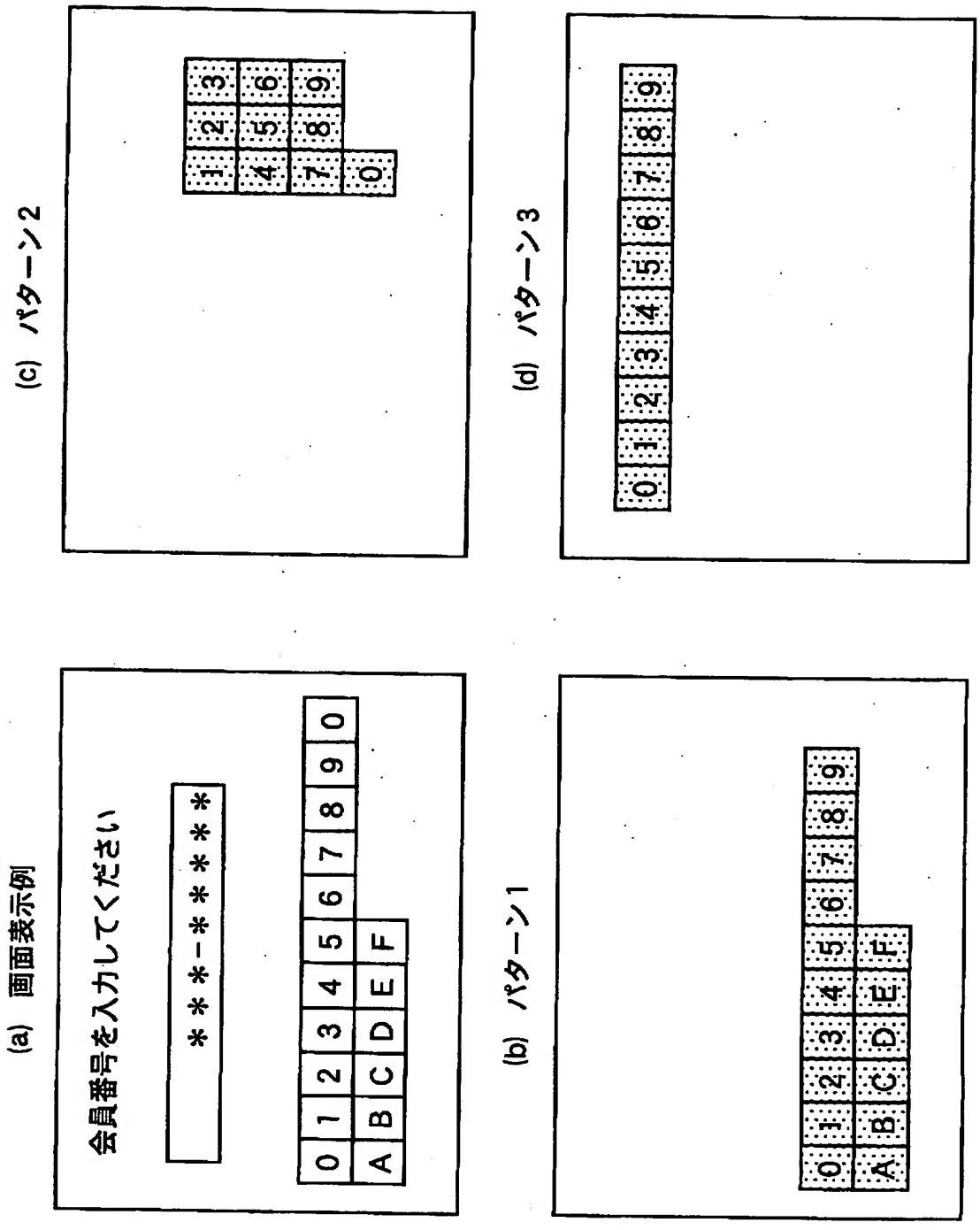
【図５】

座標範囲		関連データ
X座標	Y座標	
(10～20)	(20～40)	1
(20～30)	(20～40)	2
(30～40)	(20～40)	3
(10～20)	(40～60)	4
(20～30)	(40～60)	5
(30～40)	(40～60)	6
(10～20)	(60～80)	7
(20～30)	(60～80)	8
(30～40)	(60～80)	9
(20～30)	(80～100)	0

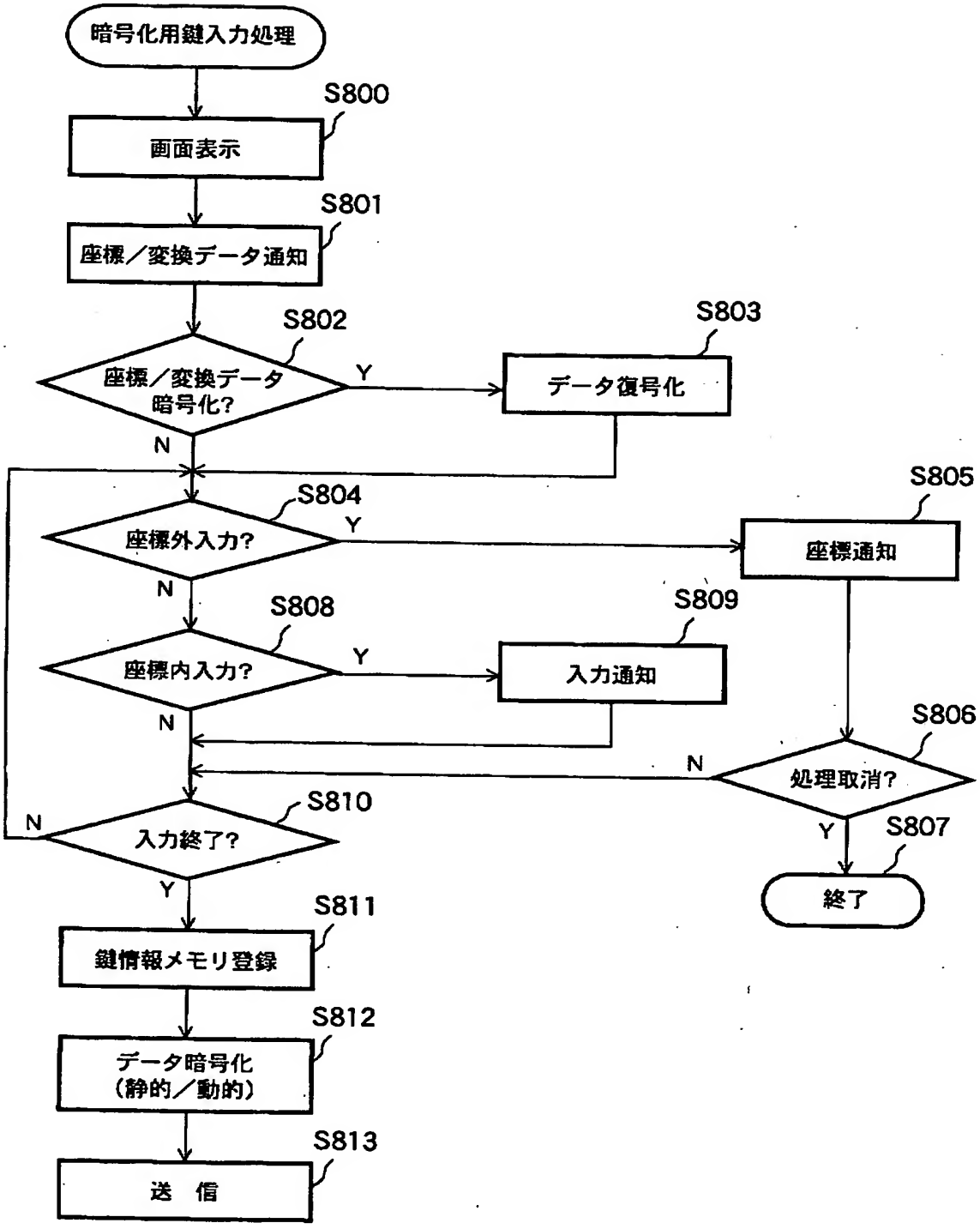
【図６】



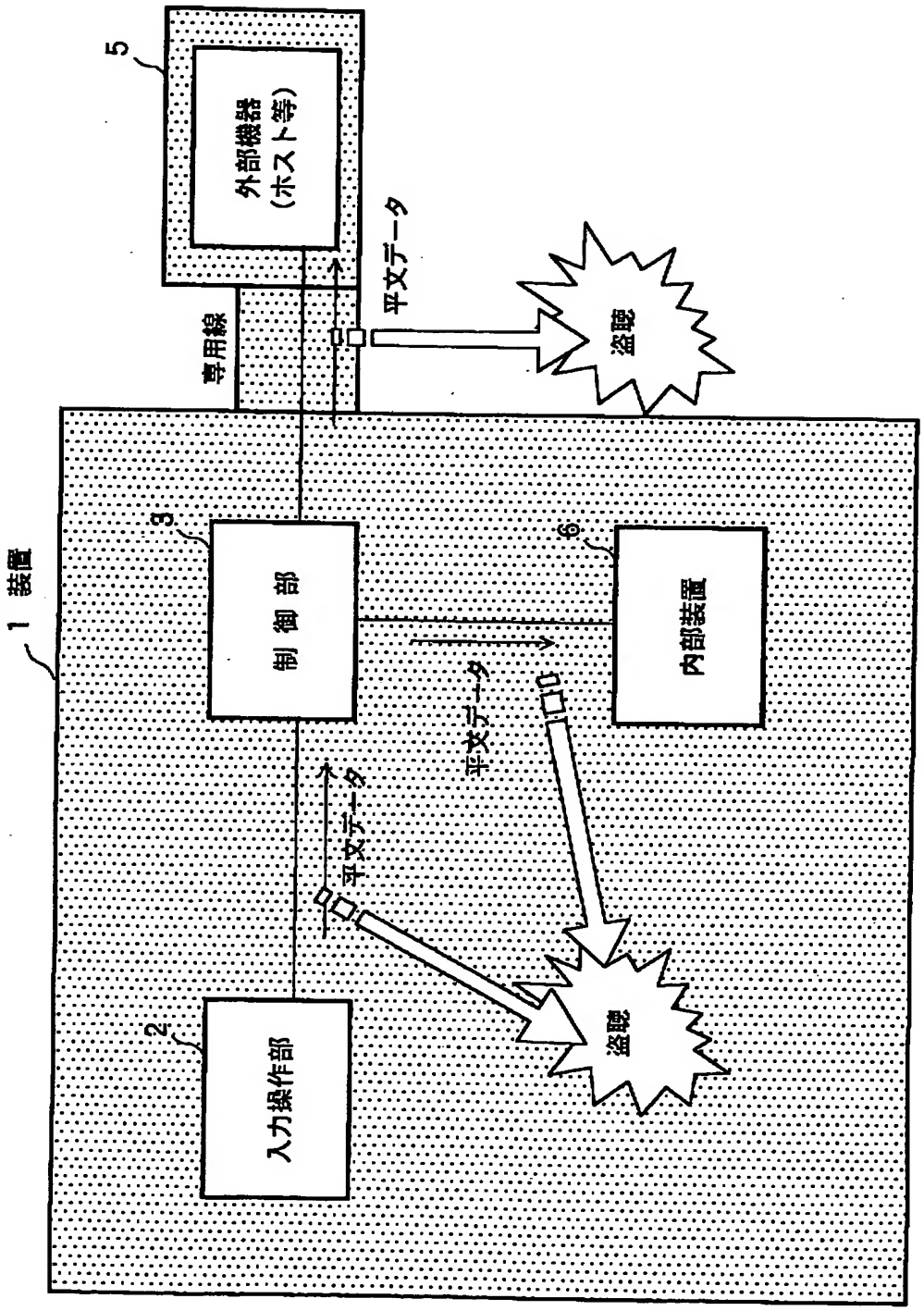
【図７】


(a) 画面表示例
会員番号を入力してください
＊＊＊－＊＊＊＊
0 1 2 3 4 5 6 7 8 9
A B C D E F
(b) パターン1
0 1 2 3 4 5 6 7 8 9
A B C D E F
(c) パターン2
1 2 3 4 5 6 7 8 9 0
(d) パターン3
0 1 2 3 4 5 6 7 8 9

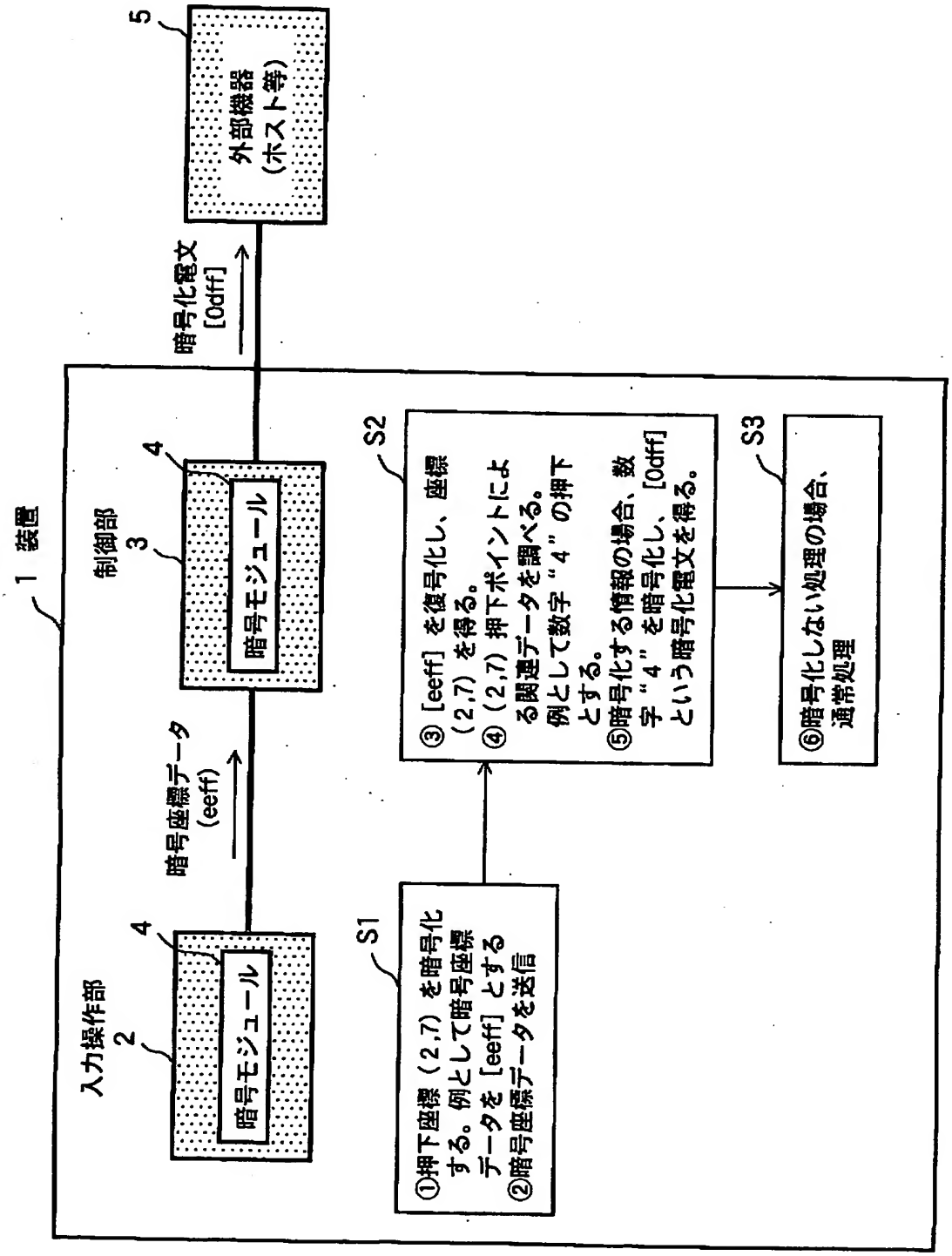
【図８】


暗号化用鍵入力処理
S800
画面表示
S801
座標／変換データ通知
S802
座標／変換データ暗号化?
Y
S803
データ復号化
N
S804
座標外入力?
Y
S805
座標通知
N
S808
座標内入力?
Y
S809
入力通知
N
S806
処理取消?
N
S810
入力終了?
N
Y
S807
終了
Y
S811
鍵情報メモリ登録
S812
データ暗号化（静的／動的）
S813
送　信

【図９】



【図１０】


1 装置
入力操作部
2
4
暗号モジュール
暗号座標データ
(eeff)
制御部
3
4
暗号モジュール
暗号化電文
[0dff]
5
外部機器
(ホスト等)
S1
①押下座標（2,7）を暗号化する。例として暗号座標データを［eeff］とする
②暗号座標データを送信
S2
③［eeff］を復号化し、座標（2,7）を得る。
④（2,7）押下ポイントによる関連データを調べる。例として数字“4”の押下とする。
⑤暗号化する情報の場合、数字“4”を暗号化し、［0dff］という暗号化電文を得る。
S3
⑥暗号化しない処理の場合、通常処理

【書類名】　　要約書

【要約】

【課題】　装置における個人情報漏洩を防ぎ、セキュリティを確保する。

【解決手段】　所定の入力操作を行う入力操作部２０と、入力操作部２０に対して所定の制御を行う制御部３０とを備えた装置１０であって、該装置１０の外部に設けられる外部装置５０とデータの送受信を行う入力操作部２０を有する装置１０において、入力操作部２０に、該入力操作部２０より入力された所定のデータを暗号化する暗号モジュール２４と、該暗号モジュール２４により暗号化されたデータを外部装置５０に送信するための送受信部２６を設けたことを特徴とする入力操作部２０を有する装置１０を提供する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００１－２５４５０９
受付番号	５０１０１２４１２１２
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１３年　８月２７日

＜認定情報・付加情報＞

【提出日】　平成13年 8月24日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社